DOCUMENT RESUME

ED 430 430 HE 031 989

AUTHOR	Sermersheim, Michael D.
TITLE	Computer Access: Selected Legal Issues Affecting Higher Education.
INSTITUTION	National Association of Coll. and Univ. Attorneys, Washington, DC.
PUB DATE	1998-00-00
NOTE	27p.
AVAILABLE FROM	NACUA Publications, One Dupont Circle, Suite 620, Washington, DC 20036; Tel: 202-833-8390; Fax: 202-296-8379; e-mail: nacua@nacua.org; Web site: http://www.nacua.org ($12).
PUB TYPE	Guides - Non-Classroom (055)
EDRS PRICE	EDRS Price MF01 Plus Postage. PC Not Available from EDRS.
DESCRIPTORS	Civil Liberties; Colleges; Computer Security; *Computers; Court Litigation; Due Process; Electronic Mail; Federal Legislation; Federal Regulation; *Guidelines; *Higher Education; *Internet; Legal Problems; *Legal Responsibility; Privacy; Universities; World Wide Web
IDENTIFIERS	*Access to Computers

ABSTRACT

This pamphlet analyzes some of the legal issues colleges and universities face in regard to faculty and student access to computers and the World Wide Web, evaluates current legal developments, and offers guidelines for developing policies for computer access. It examines sample acceptable-use standards, procedures for suspending or terminating a user's access due to violation of these standards, and due process considerations. The pamphlet goes on to discuss the vicarious liability that colleges and universities may face and the privacy expectations of computer users, noting recent court decisions related to these issues. The paper suggests that institutions need to review their computer access policies on a regular basis with counsel to keep abreast of new legal developments, and it also suggests that institutions need to educate users about their responsibilities and the effects of computer abuse. A checklist for use in drafting or reviewing computer access policies is included, along with a list of institutional resources available over the Internet. (Contains 63 footnotes.) (MDM)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

ED 430 430

NACUA

THE PUBLICATION SERIES

Computer Access: Selected Legal Issues Affecting Higher Education

MICHAEL D. SERMERSHEIM

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)
☑ This document has been reproduced as received from the person or organization originating it.
☐ Minor changes have been made to improve reproduction quality.
• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL IN MICROFICHE ONLY HAS BEEN GRANTED BY
NACUA
TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)
2B

National Association of College and University Attorneys

BEST COPY AVAILABLE

HE 031 989

NOTE: Any URL's that continue onto a second line, either in the text of the monograph or in a footnote, should be treated as one continuous address.

All URL's are accurate as August 1998, but are subject to change by the respective institutions. Should that occur, most policies can be accessed by locating the institution's homepage and searching through the table of contents, index, or other appropriate list of institutional resources.

Michael D. Sermersheim is Associate Vice President and Deputy General Counsel at the University of Akron. He is a member of the Board of Directors of NACUA and is currently serving as Chair of the Committee on Publications. Mr. Sermersheim received his B.A. and his J.D. from the University of Akron.

The author greatly appreciates the assistance of Tom Flygare, Mieke Pfaendtner, James Simon, and Linda Henderson in reviewing earlier drafts of this pamphlet.

The views expressed herein are to attributed to the author and not to the National Association of College and University Attorneys. This pamphlet is intended for general informational purposes only, and does not constitute legal advice. An attorney should be consulted regarding the specific facts and circumstances associated with any legal matter or case.

© 1998 National Association of College and University Attorneys

Printed in the United States of America

Computer Access: Selected Legal Issues Affecting Higher Education

The proliferation of personal computers over the last several decades, and their connectivity to networks, have sparked a new era for communications in the academic community. In addition to the numerous advantages brought forth by this phenomenon is the need to develop and enforce new institutional policies and practices. Projecting the application of traditional legal principles to issues surrounding computer access has raised new challenges for all members of the academic community. It is difficult to predict, in some situations, how current laws will affect the use of personal computers and their connections through the present World Wide Web network.

Sometimes mirroring and often leading changes in our society, higher education has crossed many frontiers in leaping forward into the electronic communication era. Personal computers are now linked far beyond the confines of mainframes, providing quick and easy communications that, until recently for many, were only within the realm of imagination. The benefits of electronic communication (by personal computer), however, also carry significant burdens and responsibilities.

Institutions of higher education may insist that faculty and students act responsibly in using campus-computing facilities that access other computer networks. The challenge exists in when and how to make such requirements. Drafting computer access policies requires foresight that is fair, reasonable and consistent.

A consistent policy framework for computer user access is becoming an increasingly important consideration for all colleges and universities. As such, this pamphlet analyzes some of the legal issues surrounding access to computers and to the World Wide Web within the purview of the academic community; it evaluates some of the implications of current legal developments; and it suggests guidelines for developing policies for computer access.

GENERAL CONSIDERATIONS

As computers rapidly change the landscape of information, colleges and universities should carefully, and frequently, balance their interests with the needs of faculty and students for reasonable access to computer networks. Faculty needs may entail research, course development and delivery. Students, too, may keenly appreciate the enhanced research capabilities as well as the other academic conveniences provided by computer networks.

Legislators and judges may ultimately be asked to solve issues pertaining to computer access, the outlines of which have not yet fully emerged. Higher education should take a more proactive approach in formulating future legal development by drafting and promoting fair and equitable use policies governing computer access.

Every institution has a unique approach to developing computer use policies, depending on their respective goals, mission, and user viewpoints. Local law may also cause a variety of differing considerations, as might the University's own unique culture. Regardless of these considerations, computer use policies need broad involvement in their creation to foster broad acceptance.[1]

While not exhaustive, a well-crafted computer use (or access) policy provides a general framework of user privileges and responsibilities. This may help reduce the potential for litigation and liability, as well as foster an atmosphere of collegiality between network administrators and users. The policy should be easy to read and readily available to users.[2]

An institution should initially create computer access policies to educate and communicate, to new and experienced users, the consensus of the university's culture of expectations. The policy should begin with a statement of purpose, and be accompanied by various reasons for employing the adopted policy.[3]

USERS GOVERNED

A computer use/access policy should list the individuals to whom it applies: faculty, staff, students, and guest users; and it should state clearly and concisely the standards and parameters of those who are subject to its provisions. Institutions should assess the status of each user for purposes of applying the policy. Gaps in enrollment or employment should not be a pretext for avoiding applicable use standards and penalties pertaining to those standards. In essence, the policy should apply to every person the institution serves as an Internet provider, recognizing the fact that it may be difficult to consistently and continuously enforce such a policy to all users at all times due to changes in their relationship to and with the institution. Nevertheless, an effective policy should be in place, and it should apply to all users of the system.

The policy should also reflect the resources covered: networks, standalone computers, shared computers, and connecting resources.[4]

---

1. Marjorie Hodges, as interviewed by Gary Pavela. "Developing a Computer Use Policy." *Synthesis: Law & Policy in Higher Education*, Vol. 7, Number 4, (Spring 1996).

2. "Setting Up a Corporate Policy for Internet Use: A Checklist." 6 *Computer Law Strategist* 4, 12 (1995).

3. Examples of sample policies can be found at the following URL sites: Using Computer Resources at Brown University, http://www.brown.edu/webmaster/tm009.html; University of Michigan Information Technology Policies and Guidelines, http://umich.edu/~policies/; http://umich.edu/~policies/usepolicy.html; http://www.umich.edu/~policies/responsible-use.html; Responsibilities of all New York Users, http://www.nyu.edu/resnet/NYU-responsibilities.html; Stanford - Residential Computing Acceptable Use Policy, http://rescomp.stanford.edu/use.html; University of Pennsylvania, http://www.upenn.edu/computing/help/doc/passport/policies.html; University of Florida, http://www.circa.ufl.edu/comp.netpolicy.html; The University of New Mexico, http://unm.edu/cirt/info/general/ethics.html, subject to change without notice; Loyola University of Chicago, http://www.luc.edu/infotech/sae/newuse.html.

4. See University of Tulsa, "Computer Ethics Policy," URL: http://centum.utulsa.edu/ethics.html. This policy applies to the use of all institutional data regardless of the office in which it resides or the format (paper, film, electronic, etc.) in which it is used.

STATEMENT ON ACCEPTABLE USE STANDARDS

A Florida State law professor and the Director of the Florida Information Research Center note that institutions of higher education "may draft acceptable use policies and publish them as contracts in which users are made aware of reasonable restrictions applicable to access and use of the system."[5] These authors note that "[a]n institution may expressly disassociate itself from the communications of its users."[6] They urge requiring users to sign a use agreement, which contains a notice of responsibility for proper use,[7] and which may provide a whole host of acceptable (or prohibited) uses. While this type of agreement may strive to educate users about acceptable standards of computer use and etiquette, it should not serve as a one-time solution for all users. Education about acceptable usage and standards for network access should be continuous.

An institution cannot expect cooperation with computer use guidelines unless it first provides a clear understanding of expectations. Standards of what is and is not acceptable provide a model for users and administrators in their use of computers, enforcement of institutional policy, and fulfillment of their educational mission. Moreover, courts may set aside a suspension or termination of computer access privileges where there appears to be a denial of due process or arbitrary action on the part of the administration. Absent a clear statement of expected (and prohibited) uses, a court may find a revocation of network privileges to be unfair.[8]

A computer use *Bill of Rights* arose from an American Association for Higher Education (AAHE) program called the "Ethics and Technology Initiative."[9] This document provides general guidance in drafting a fundamentally fair balance of considerations for institutions and for faculty, staff, and student users. The model proposes that users (called citizens) be afforded fundamental rights in computer access.[10] The model rights include: access that would not be denied or removed without just cause; appropriate training and tools to effect access; and the right to be informed about personal information that is or has been collected about the user, to review and offer correction of the information and the assurance that the information shall not be used for other than the express purpose of its collection without permission from the user.[11]

---

5. J. Peckham and W. Scmid. "Forum Analysis in Cyberspace: The Case of Public Sector Higher Education." *West Education Law Quarterly*, 470 (1995).

6. *Id.*

7. *Id.*

8. It is impractical and impossible in this pamphlet to provide a complete review of the various levels of due process afforded individuals undergoing loss of privileges in academe. For a more complete discussion, see William Kaplin & Barbara Lee, *The Law of Higher Education*, at 290-94, 462-64, 484-500 (3rd ed. 1995).

9. URL: **http://www.luc.edu/infotech/sae/bill-of-rights.html**. The principal architect for the *Bill of Rights* is Dr. Frank W. Connolly, an associate professor at American University in Washington, DC. He can be contacted by e-mail at frank@american.edu.

10. *Id.*

11. *Id.*

The institution may place responsibilities on users as a condition of their utilizing computing facilities and equipment. Colgate University, for example, provides for an "Agreement for Use of Computing Facilities,"[12] which informs prospective users that they are permitted to use various Colgate computing facilities as long as the use does not violate applicable Colgate license agreements, policies, standards, and governing laws.[13] In this regard, it is suggested that institutions consider referring to computer access as a privilege, not a right. An example of this approach is Indiana University.[14]

As yet another example, Cornell University provides a thorough statement of responsible use expectations for users, and clearly specifies the procedures following a violation.[15] The benefit of having such a specific policy is that it enables the institution to respond consistently to complaints about computer misuse.[16]

By way of illustration, a sample statement of prohibited uses might include:

1. Harassment by use of computing facilities.
2. Violation of the privacy of others.
3. Destruction or damage to equipment, software, or data belonging to the university or others.
4. Disruption to or performing unauthorized monitoring of electronic communications.
5. Violation of computer system security.
6. Use, without authority, of computer accounts or access codes.
7. Use of computing facilities for purposes unrelated to the mission of the university.
8. Violation of copyright and software license agreements.
9. Academic dishonesty, such as plagiarism and scientific misconduct.
10. Violation of applicable university policies including, but not limited to, sexual harassment, student disciplinary procedures, access and use of computing, networking, telephone, and information resources, etc.
11. Commitment of crimes or prohibited acts. Illegal acts involving

---

12. Colgate University. URL: ftp://ftp.unm.edu/ethics/ColgateU.policy

13. *Id.*

14. See Indiana University's statement on "Computer Users' Privileges and Responsibilities;" URL: http://www.indiana.edu/~ucspubs/iu001/

15. "Responsible Use of Electronic Communications," Cornell University Policy Library – Policy 5.1; originally issued April 1994, revised October 1995; URL: http://www.univco.cornell.edu/policy/RU.for.html

16. Hodges, *supra*, note 6, at 554.

university computing facilities may also be referred to state and federal authorities for prosecution.

Other institutions' policies prohibit:

1. Inappropriate mass mailing, which includes mailings to news groups, mailing lists, or individuals, e.g. spamming, flooding, or bombing.[17]
2. Knowingly or carelessly running or installing on any computer system or network, or giving to another user, a program intended to damage, or to place excessive load on a computer system or network. This includes programs known as computer viruses, Trojan Horses, and worms.[18]
3. Engaging in activity that does not comply with the Honor Code or with the principles of the Church of Jesus Christ of Latter Day Saints...to store or transfer pornography.[19]
4. Personal use that creates a direct cost for the University.[20]
5. Spoofing – or constructing an electronic mail communication so it appears to be from someone else.[21]
6. Snooping – or obtaining access to the files or electronic mail of others for the purpose of satisfying idle curiosity, with no substantial University business purpose.[22]
7. Electronic communication that is repeated and unwanted, as such action may constitute harassment. Communication targeted at a specific individual with the intent to harass or threaten is a violation, for example, of the Cornell policy. According to the policy, a user who receives unwanted e-mail or other forms of communication, may want to notify the sender that the communiques are unwanted. (In some instances, the sender may not realize that his or her communication is unwanted unless he or she is told.) If the sender continues to communicate after being placed on notice, or if the recipient feels uncomfortable confronting the sender, the policy stipulates that the incident should be reported to the Office of the Judicial Administrator. The Cornell police are also to be contacted if the situation is potentially serious and requires immediate attention. All parties involved should save electronic copies of anything that can be used as evidence.[23]

---

17. The University of California at Davis, URL: http://www.ucdavis.edu/AUP.html
18. *Id.*
19. Brigham Young University, URL: http://www.byu.edu/cougarnet/policy.html
20. University of Colorado, URL: http://www.cusys.edu/~policies/General/email.html
21. *Id.*
22. *Id.*
23. Cornell University: URL: http://www.cornell.edu/Computer/responsible-use/Index.html# hate-speech

8. Posting hate speech – defined as uncivil, antagonistic, or derogatory speech that is disrespectful of classes of people. Although hate speech may be extremely offensive to members of the targeted group, Cornell acknowledges in its use policy that posting hate speech on the web does not generally constitute a violation of Cornell policies. This is due to the fact that, as an educational institution, Cornell is committed to protecting freedom of expression, yet reserves the right to decide that hate speech directed to classes of individuals may present a hostile environment warranting certain restrictive actions.[24]
9. Deliberately attempting to degrade the computer systems, networks, or personal computer performance, or depriving other users of the resources of, or authorized access to, any college or individually owned computer.[25]
10. Using loopholes in the Dartmouth computer systems and network, or knowledge of a special password, should not be used to damage computer systems or networks, to obtain unauthorized resources, or to take resources from other users.[26]
11. Resorting to unethical or irresistible use of a computer by using computer facilities for work done on behalf of a commercial firm, and unplugging or reconfiguring computer equipment to make it unusable or difficult to use.[27] (See also Nassau Community College, *supra*,... using the College systems for commercial or profit-making purposes without written authorization from the college administration.)
12. Accessing another individual's account, private files, or e-mail without permission of the owner.[28]
13. Misrepresenting one's identity in electronic communication.[29]
14. Using the University's trademarks, logos, insignia, or copyrights without prior approval.[30]
15. Using computer resources for any other purpose which is illegal, immoral, unethical, dishonest, damaging to the reputation of the University, or likely to subject the University to liability....[31]
16. The University of Pittsburgh prohibits: "Using a computer, computer system, computer network, or any other University

---

24. *Id.*
25. Dartmouth College, URL: http://www.dartmouth.edu/comp/comm/citbook/compcode.html.
26. *Id.*
27. James Madison University, URL: http://www.jmu.edu/JMUpolicy/1207.htm.
28. Nassau Community College, URL: http://www.sunynassau.edu/policies/labpol.htm.
29. *Id.*
30. Notre Dame University, URL: http://www.nd.edu/~doc/General/G0001.HTML.
31. *Id.*

property for the purpose of devising or executing a scheme or artifice with the intent to defraud, or for the purpose of obtaining money, property, services, or any other property of value by means of false or fraudulent pretense or representation is prohibited."[32]

17. Finally, the University of Missouri simply proclaims: "Compute unto others as you would have them compute unto you."[33]

Public institutions may not be able to enforce certain of these provisions, if adopted, due to constitutional constraints.

See also other use statements from such institutions as the University of Tulsa (http://centum.utulsa.edu/ethics.html); Arlene Rinaldi's Netiquette Home Page (http://rs6000.adm.fau.edu/~rinaldi/netiquette.html); and University of Delaware (http://www.udel.edu/eileen/Ecce/policy.approved.html).

SUSPENSION OR TERMINATION OF ACCESS

The Internet is fast becoming an extremely effective communication tool, considered by some as "the ultimate tool of education, as well as democracy."[34] Many faculty, staff, and students use the resources of the Internet heavily to conduct research, communicate with others, conduct and complete course documents and tests, and post information to networks and bulletin boards on a broad range of subjects. The application of computer networking, arguably, will greatly expand as the technology continues to evolve, and as users increase in number and frequency.

Consistent with this increased use will be a greatly increased need to ensure that even the most temporary suspension of computer access privileges is not unfair, arbitrary, or unwarranted. System operators will face increased responsibility in assuring they do not wrongly preclude faculty and students from teaching, learning, and performing research. Suspension or termination of a student's computer access could feasibly result in an academic failure, which, in turn, could trigger an academic suspension or dismissal. Tenured faculty, who base their instruction on computer networking, could find themselves precluded from fulfilling the terms of their contract with the institution. The significant impact of interfering with computer access, therefore, becomes more and more clear.

Consider the following hypothetical: A creative faculty member offers lectures and course materials to students through a web page on the Internet. The course, offered in this fashion, is essential to students in the department. The faculty member is accused of wrongfully using a university computer and Internet connection. A diligent network administrator,

---

32. University of Pittsburgh. URL: http://www.pitt.edu/DOC/94/271/42590/policies/10/10-2-05.html.

33. University of Missouri. URL: http://www.missouri.edu/iats/faculty/policies.shtml.

34. Richard A. Detweiler. "Democracy and Decency on the Internet." *The Chronicle of Higher Education*, June 28, 1996.

desiring to act promptly, suspends the web page and the faculty member's privileges for the alleged incident late on a Friday afternoon. Access is denied between the faculty member and students for course work to be completed during the weekend; consequently, students for the particular course are not able to post their assignments to the suspended web page. The scenario could be further complicated if the particular weekend was at the end of an academic term. Grades of students could be delayed, potentially affecting their ability to graduate or register for other courses in the sequence.

The ramifications arising from this vignette are vexing for the faculty member, the students, and the University. In a worst case – albeit not inconceivable – scenario, the faculty member may be damaged from adverse publicity and stigma (or perception of others) about the incident. He or she could also be hurt professionally within the department where he or she may be seeking promotion, retention or tenure. The students may be precluded from completing a course in sequence necessary for graduation, potentially affecting future employment. The system administrator may be subject to criticism for such a stringent action, particularly if the allegations cannot be substantiated. The University faces embarrassment over such an incident, not to mention possible claims for damages from affected individuals.

To this end, institutions should carefully assess who terminates access privileges and how termination is effected. A policy that seeks to educate users about prohibited computer misconduct, strives to achieve fairness and consistency in termination practices, and tailors the penalty to the misdeed, will have a better chance of garnering campus acceptance, as well as surviving potential judicial scrutiny. For public institutions, there is a greater need to provide some degree of due process prior to computer privilege suspension or termination. Arguably, the policy should initially provide for assumptions of innocence and potential mistake. Only after due deliberation of all pertinent facts and consequences should any action be taken to interrupt computer access privileges except in bona fide emergencies.

WHAT PROCESS IS DUE?

Courts generally afford latitude to public institutions of higher education in drafting and upholding regulations about student conduct. Private institutions have even greater flexibility. In the often-cited *Esteban v. Central Missouri State College*,[35] the U.S. Court of Appeals for the Eighth Circuit stressed the need for flexibility and reasonable breadth, rather than meticulous specificity, in college student conduct regulations.

Similarly, when colleges and universities draft computer access policies, they need to determine how best to educate users about their policies, and

35. 415 F.2d 1077 (8th Cir. 1969).

they need to take into consideration how all individuals – not just the person who has violated the policy – will be affected by privilege termination. Cessation of computer privileges, as outlined above, naturally will have different effects on different individuals.

Generally, the degree of the privilege being reviewed for revocation dictates the amount of due process afforded the affected individual (before the privilege is revoked). This is a phenomenon, in particular, for public colleges and universities, acting as state institutions. For example, a more stringent analysis is applied to the requirements of due process in a tenure revocation.[36] Different standards of due process are required in student disciplinary matters than in academic matters.[37] Academic assessment bears little semblance to traditional judicial and administrative fact finding hearings.[38]

It is important that both public and private institutions develop specific grounds and procedures for terminating computer access privileges. The policy at Indiana University, for example,[39] provides for termination under the following circumstances:

1. Unused accounts for 30 days.
2. Discontinuing students or graduating students. After one semester, if student has either graduated from Indiana University or is discontinuing his/her education at Indiana University for one or more semesters.
3. Employee Resignation (after 30 days).
4. Terminated Employees (after 30 days).
5. Computer Abuse Sanction. After due process, if the relevant University office, i.e., Dean of Students, Dean of Faculties, Human Resources, etc., determines that computer account abuse necessitates loss of computing account privileges.

Cornell University, a private institution, has provided for much greater specificity in its policy on "Responsible Use of Electronic Communications."[40] More specifically, the policy provides detailed guidance as to what constitutes a violation, who should file a complaint, where the complaint should be filed, and what action should be generated on the complaint.

As a general rule, most new users, and even some experienced users, can be expected to violate some computer use rule. Most of the violations may be innocent and harmless mistakes. Institutional policies, and those

---

36. Kaplin & Lee, *The Law of Higher Education* at 288-93 (3d edition, 1995).

37. *Board of Curators of the University of Missouri v. Horowitz*, 435 U.S. 78 (1978).

38. See *Regents of the University of Michigan v. Ewing*, 474 U.S. 214 (1985), relying upon *Horowitz* to instruct that judges should show great respect for faculty judges in academic matters.

39. "Termination of Computer Accounts," Indiana University, URL: http://www.indiana.edu/~ucspubs/iu001/

40. Cornell University, URL: http://www.univco.cornell.edu/policy/RU.for.html

charged with enforcing the policies, should make very effort to appreciate these mistakes, and give violators the benefit of the doubt. Consider the following sample language that seeks to reduce most infractions to the least serious penalty:

> Every attempt shall be made to impose non-punitive sanctions or impose the least serious penalty, except where serious violations warrant more serious sanction. Warnings are generally to instruct users who may be prone to mistakes, especially while learning new software. Warnings should be considered as a guide to users to assist them in their use of University informational resources. Privilege suspension shall only be used for more serious or repeated violations of pertinent University rules, regulations, and directives.
>
> Sanctions may generally be classified under the following:
>
> 1. Warning. Warning users of violations (transmitted electronically or in writing to the user).
> 2. Temporary suspension. Temporarily denying access or suspending usage, based on seriousness of the violation or recurrent violations of other prohibited access and use standards.
> 3. Suspension for a definite time.
> 4. Termination of access and privileges for an indefinite time.

Following a theory of graduated penalties (with greater penalties being used for more serious or repeated infractions), institutions should endeavor to attach a comparably graduated level of due process, based upon the level and severity of the computer misconduct. While simple warnings may necessitate only electronic communication between a system operator and an offender, suspension and privilege termination should warrant greater procedural safeguards. If a graduate student's access privileges are terminated, thereby precluding course or dissertation fulfillment, the effect can arguably be the same as a disciplinary suspension. The degree of due process, therefore, should be modeled after, or linked with, the applicable disciplinary code that would otherwise apply to that student. This same scenario would also be appropriate to undergraduate programs where computer access is, or becomes, essential to successful completion of courses.

In the case of a tenured faculty whose computer access privileges are recommended for termination, the institution would be well served to incorporate a process similar to that discussed above, which allows for graduated discipline and cessation only after a hearing. Indeed, a serious penalty such as access termination or suspension during the semester, which then precludes the faculty member from finalizing a course, adversely affects not only that faculty member, but all of the students in the course. If access is terminated for a minor infraction, or without any

meaningful process, the institution may be subject to judicial intervention, review of its policy, and revision by fiat from a court.

It may be even more troubling if the privileges of a faculty member are terminated, thereby affecting the faculty member's retention, tenure and promotion ("RTP"). Absent a well-constructed policy governing these situations (and incorporating appropriate institutional rules on RTP), there is the potential for constructive discharge if the faculty member is unable to perform teaching duties.

The University of Delaware policy, for example, directs enforcement pursuant to an appropriate disciplinary code applicable to the individual.[41] It furthermore requires that alleged computer misuse violations be processed according to various applicable judicial processes outlined in the *University of Delaware Policy Manual*, the *Personnel Policies and Procedures for Professional and Salaried Staff*, the *Faculty Handbook*, *University Collective Bargaining Agreements*, and the *Official Student Handbook*. The policy also states that access and use violations are treated seriously, potentially warranting prosecution under specific criminal statutes or other appropriate laws.[42]

As an institution begins drafting or revising its computer use/access policies, care should be taken to similarly review other policies that may be incorporated, by reference, into the access policy. In addition, student conduct codes, personnel policies, and faculty handbooks all should be reviewed to ensure that they include reference to alleged computer infractions. A careful blending of these policies will no doubt at least provide for a more equitable and acceptable process.

At a minimum, all institutions (public, because they are required to do so, and private, because it is simply "good practice") should consider adopting the following basic principles when developing a suspension and termination procedure affecting an individual's Internet access:

1. Adequate notice to the individual of the alleged infraction.
2. An opportunity to respond to the allegation.
3. Adjudication of suspension and termination decisions by an individual or individuals separate from the system operators.
4. Opportunity to appeal an adverse decision.

Immediate termination or suspension of privileges should be reserved only for the most serious situations where injury to others, or system or property damage, are probable. Unless necessary to protect others or system integrity, suspension or termination should only be effected after the individual has been afforded the appropriate level of due process.

---

41. "Policy for Responsible Computing," University of Delaware, URL: http://www.udel.edu/eileen/Ecce/policy.approved.html.

42. See also, "Computer User's Privileges and Responsibilities," section on "Sanctions," Indiana University, URL: http://www.indiana.edu/~ucspubs/iu001/.

Additional safeguards should be considered for more serious cases where the penalty might have a more adverse affect on the individual.

VICARIOUS LIABILITY: PUBLISHER OR DISTRIBUTOR?

Vicarious liability is the responsibility of one for the actions of another. An employer is generally considered liable for the actions of an employee when that employee is acting within the scope of employment. The employer is accountable for an employee's negligence if it had control over the actions of the employee. Typically, the employer and the employee are named defendants in a lawsuit.

The accountability of institutions of higher education for the actions of contentious students, disgruntled employees, and others accessing the institution's computer networks, poses some serious and, in some instances, conflicting concerns. Obviously, with the tools to expand communication, facilitate public forums on a myriad of issues, and the potential for increased connection of users across the globe, institutions are hardly in a position, from either a policy or practical standpoint, to screen the comments of users. Nonetheless, two cases have raised to the forefront the issue of vicarious liability of electronic computer communications.

Cubby, Inc. brought an action against CompuServe, a provider of an online general information service or electronic library that subscribers access from personal computers.[43] Cubby, Inc. alleged that another user made libelous and defamatory remarks about Cubby and its partners through a journalism forum hosted by CompuServe. Alleging that CompuServe was a publisher of the information to other users, rather than a mere distributor, Cubby sought relief from CompuServe for the remarks.

In a summary judgment in favor of CompuServe, the court noted two important factors: CompuServe had no opportunity to review the material before its contents were circulated to other users; and CompuServe had no notice of any complaints about the contents of the publication or the person making the statements about Cubby.[44]

The District Court found that CompuServe was a distributor, not a publisher; therefore, it had no duty to screen the material. As a distributor, CompuServe was not liable since it had no prior notice of the allegedly defamatory material.

The decision reached in *Stratton Oakmont, et. al. v. Prodigy Services Company, et. al.*[45] is more bothersome. In *Stratton Oakmont*, the communicator of the allegedly libelous remarks was not known. Prodigy, an electronic online service provider, was held to the standard of a publisher with vicarious liability for the comments of a user who was not known or

43. *Cubby, Inc. v. CompuServe*, 776 F.Supp. 135 (S.D.N.Y. 1991).

44. *Id.* at 137.

45. 65 USLW 2765, 23 *Media L Rep.* 1794 (S.Ct. 1995).

found.[46] This is partly due to the fact that Prodigy, unlike CompuServe, marketed itself as a family-oriented computer network, and held itself out to the public as an online service that exercised editorial control over the content of messages posted on its computer bulletin boards.[47] Prodigy was also noted to have:

- Promulgated message content guidelines;
- Used a software screening program to prescreen all bulletin board postings for offensive language;
- Used bulletin board leaders to enforce the guidelines; and
- Provided board leaders with an emergency delete function tool to remove a note and send an explanatory message.

The Court in the *Stratton Oakmont* case was not persuaded with Prodigy's argument about the sheer unfeasibility of manually screening over 80,000 messages per day (as of the time of that case).[48] In concluding that Prodigy was a publisher and not a distributor, the Court emphasized two distinctions between Prodigy and CompuServe: Prodigy held itself out to the public as controlling message content, and it implemented this policy through software and board leaders.[49]

The Communications Decency Act of 1996 (CDA)[50] seeks to provide a defense to online service providers who attempt to screen patently offensive sexual material to individuals under the age of 18. This new section purports to provide a *Good Samaritan* exception to service providers who also attempt to screen offensive materials from minors. In essence, this type of defense seeks to shield a provider if it attempts, but fails, to successfully bar access to the offensive material. The statute indicates, in effect, that the provider shall not be treated as a publisher of the material, nor shall it be held liable for any action voluntarily taken to restrict access of minors to obscene materials. One purpose of the CDA is to overrule *Stratton Oakmont v. Prodigy* and any other similar decisions that have treated Internet service providers and users as publishers rather than distributors of content that is not their own, or because they have restricted access to objectionable material.[51]

Whether the CDA and/or emerging case law will continue to embrace this distributor/publisher dichotomy is uncertain. The CDA will, no doubt, undergo further legal challenge. At this juncture, institutions may find it safer to make more general statements in their policies about prohibiting

---

46. *Id.*
47. *Id.*
48. *Id.*
49. *Id.*
50. 47. U.S.C. § 230.
51. *See* the *U.S. Congressional Record* at 142 *Cong. Rec.* H1078, H1136.

criminal acts. Further, institutions may desire to explicitly note that they do not purport to control the content of e-mail and electronic materials.

Two cases construing the Communications Decency Act are noteworthy: *Zeran v. America Online, Inc.*[52] and *Doe v. America Online, Inc.*[53] Plaintiff Zeran alleged that America Online (AOL) negligently distributed a series of fake messages, posted by another person. The messages caused harm to Zeran and his business by attributing his name and number to a gleeful reaction about the Oklahoma Bombing incident. Zeran contended that, upon notifying AOL of the existence of these messages, AOL had a duty to remove the objectionable messages immediately and preclude further postings of the messages. Unable to preclude posting of more of the messages, AOL could only remove the messages of which it received notice.

The Court dismissed Zeran's claim, and held that the *Good Samaritan* provision of CDA pre-empted the lawsuit. The Court noted that Zeran's attempt to impose distribution liability on AOL was essentially an attempt to treat AOL as a publisher of the defamatory material, when in fact AOL was simply a distributor. Section 230(c)(1) of CDA preempts treating AOL as a publisher.[54] The Court further iterated that the negligent distributor theory is merely a facet or type of liability for publishing defamatory material.[55]

Doe v. AOL[56] seems to further extend *Zeran* by holding that the CDA pre-empted a claim by a parent on behalf of a minor for alleged negligence in permitting a subscriber to post messages depicting the minor in pornographic pictures and videotapes. The Court held that AOL is not required to monitor, screen, and censor great volumes of information transmitted by third parties over its system.

Many college and university Internet providers may have, or typically exercise, less control over the content of their systems. As mere providers of access (or space on a hard disk of a remote computer), and subject to First Amendment constraints, colleges and universities, arguably, should not be liable for the content of the electronic communications of system users. According to a noted authority, colleges and universities should not even be subject to a distributor standard of liability.[57]

Certainly, local counsel should be consulted on these issues. Since this area of the law presently is not well settled, institutions should weigh the ramifications of their actions carefully in situations where they are notified that materials placed on their systems by others are offensive, pornographic, or libelous. Public institutions, in particular, may be subject to challenge as restraining free speech of users. However, both public and private

52. 958 F. Supp. 1124 (E.D. Va.), *aff'd.* 129 F. 3d 327 (4th Cir. 1997).

53. 1997 Fla. App. LEXIS 7606.

54. *Id.* at 1133.

55. *Id.*

56. *Id.*

57. Steven J. McDonald, "An Overview of Internet Law," presented at the *19th Annual Conference on Law and Higher Education*, February 11, 1998).

institutions face challenge with faculty for potential restriction of academic freedom.

Once a college or university knows, or has reason to know, that the material sent over the Internet is defamatory or criminal in nature, it should consider whether to implement procedures to block and/or remove the material. Obviously, campus officials may want to include relevant constituencies in such a decision, bearing in mind institutional culture, mission statement (to the extent it is incorporated into any use or web page policy), and other policies that may impact such a decision.

The University of Delaware uses the following statement in this context:

> The University will not impose any restraints on, nor make any effort to monitor the content of, communications other than those imposed by applicable Federal, State, or local laws, including laws regarding the right to privacy and laws which prohibit defamatory material. Users of the University's information systems are advised that their communications are subject to such laws and that the consequences of violations can be severe.[58]

PRIVACY EXPECTATIONS

Lacking a specific policy focusing on a reduced expectation of privacy in the work-place, a court may in fact impose such an expectation – where facts lead to a conclusion that employees reasonably expect their desks (and possibly their hard disks) to be free from employer searches. In *O'Connor et. al. v. Ortega*,[59] the United States Supreme Court found a reasonable expectation of privacy for a physician regarding his desk at a hospital. The Court noted that "there was no evidence that the hospital had established any reasonable regulation or policy discouraging employees... from storing personal papers and effects in their desks or file cabinets."[60] The Court further indicated that the reasonableness of privacy, and the appropriate standard for a search, may vary according to the given context. Consequently, it is important to delineate the boundaries of privacy in the work-place.[61]

Users may perceive that any information they transmit or receive over a college or university computer network is personal and confidential. Absent a policy statement to the contrary, there is little reason for them to assume otherwise. Institutions should be aware of this expectation, and provide an appropriate policy statement as to the institution's position about the privacy of electronic communications. Institutions should also consider developing a policy statement that notifies the user that there may not necessarily be an expectation of privacy attached to their electronic com-

---

58. "Policy for Responsible Computing," University of Delaware, URL: http://www.udel.edu/eileen/Ecce/policy.approved.html.

59. 480 U.S. 709 (1987).

60. *Id.* at 719.

61. *Id.* at 715.

munications, and that the institution reserves the right to examine files where there is a reasonable suspicion of wrongdoing or computer misconduct.[62]

Those institutions governed by public records laws should also notify users of the impact of such laws on their electronic mail. The University of Florida provides the following such statement in its "Policy on Public Records Law and E-mail:"[63]

> E-mail created or received by University of Florida employees in connection with official business, which perpetuates, communicates or formalizes knowledge, is subject to the public records law and open for inspection.
>
> If your e-mail falls within the definition of a public record, you may not delete it except as provided in the university's record retention schedule[.]

SUMMARY

The emergence of computers and their growing importance to education will continue to pose potential challenges and disputes for institutions and users dependent on network capability. Well-crafted policies may aid in avoiding pitfalls that may arise in the evolution of computer networking. However, it is not enough for institutions to merely draft a policy and consider the work completed; rather the policies should be reviewed on an on-going basis with legal counsel, and certainly upon the occasion of new legal developments. The law has only just begun to develop in this area. Effective computer access policies should allow for an institution to determine for itself various aspects of computer use within the institution (rather than having regulators from outside the institution do so).

Equally as important as the development and review of computer usage policies is the need to educate users about their requirements, and the need for responsible computer behavior. Colleges and universities educate others about a broad range of fields, not the least of which should include campus expectations about computer usage, the effects of computer abuse, and the need to act responsibly so as to avoid intrusion by others in the expansion of this evolving communication tool. To the extent that academe does not provide its expertise in this development, education, and review, courts and legislators may be inclined to provide directives and regulations on our behalf.

---

62. *See* University of Florida's policy statement on this topic: URL: http://www.circa.ufl.edu/handouts/services/policy/policy.html#toc5, which provides that: "Within the limits of the capability of the computer system, CIRCA will attempt to maintain the privacy of your files and electronic mail. However, CIRCA has the right to examine any file, backup archive, electronic mail, or printer listing as part of normal system administration or when there is a reasonable reason to believe a user is violating policies specified in this document." *See also*, Colgate University's "Agreement for Use of Computing Facilities" at URL: ftp://ftp.unm.edu/ethics/ColgateU.Policy

63. University of Florida, URL: http://www.ufcn.ufl.edu/email.htm

CHECKLIST

The following checklist may be helpful in providing a framework for drafting and/or reviewing a computer use/access policy. At a minimum, such a policy should:

1. Provide a consistent framework for computer user access.
2. Be easy to read and readily available to users.
3. Educate and communicate to new and experienced users the consensus of the university's culture of expectations.
4. List the individuals to whom it applies: faculty, staff, students, and guest users.
5. Indicate the resources covered: networks, stand-alone computers, shared computers, and connecting resources.
6. Disclaim communications of its users, particularly in regard to personal web pages.
7. Require users to sign a use agreement, which contains a notice of responsibility for proper use.
8. Clearly state the rights and responsibilities of users, including prohibited uses.
9. Provide training to users about the policy and expectations about computer use.
10. Carefully weigh the impact of suspending one's computer privileges. Even the most temporary suspension of computer access privileges can be potentially harmful to a user.
11. Consider basic safeguards when developing a suspension and termination procedure, such as:
    - Adequate notice to the individual of the alleged infraction;
    - An opportunity to respond to the allegation;
    - Adjudication of suspension and termination decisions by an individual or individuals separate from the system operators;
    - An opportunity to appeal an adverse decision;
    - Immediate termination or suspension of privileges should be reserved only for the most serious situations where injury to others, or system or property damage, are probable.
12. Consider following a theory of graduated penalties (with greater penalties being used for more serious or repeated infractions). Care should be taken to similarly review other policies that may be incorporated by reference into the access policy.

13. Train system administrators about suspension and due process requirements.
14. Consider developing a policy statement that notifies users that there should not necessarily be an expectation of privacy attached to their electronic communications, and that the institution reserves the right to examine files where there is a reasonable suspicion of wrongdoing or computer misconduct.
15. Consider adopting an appropriate variation or facsimile of the following statement from the University of Delaware:

    The University will not impose any restraints on, nor make any effort to monitor the content of, communications other than those imposed by applicable Federal, State or local laws, including laws regarding the right to privacy and laws which prohibit defamatory material. Users of the University's information systems are advised that their communications are subject to such laws and that the consequences of violations can be severe.
16. Review policies on an on-going basis with an emphasis on education.

Institutional Resources Accessible by URL*

Institution:	*Resource and URL Reference:*
Brown University	Using Computing Resources at Brown University http://www.brown.edu/webmaster/TM009.html
University of Michigan	Information Technologies Policies and Guidelines http://www.umich.edu/~policies/ http://umich.edu/~policies/usepolicy.html http://www.umich.edu/~policies/responsible-use.html
New York University	Responsibilities of NYU Users http://www.nyu.edu/resnet/NYU-responsibilities.html
Stanford University	Residential Computing Acceptable Use Policy http://rescomp.stanford.edu/use.html
University of Pennsylvania	Policy on Acceptable Use of Electronic Resources http://www.upenn.edu/computing/help/doc/passport/policies.html
University of Florida	Computing Policy, Planning and Management Homepage http://www.circa.ufl.edu/comp.netpolicy.html
	Proper Use of Computing Facilities http://www.circa.ufl.edu/handouts/services/policy/policy.html#toc5
	Policy on Public Records Law and E-mail http://nervm.nerdc.ufl.edu/UPDATE/U951001a.HTML http://www.ufcn.ufl.edu/email/htm
The University of New Mexico	University of New Mexico Ethics Code and Acceptable Use Policy http://www.unm.edu/cirt/info/general/ethics.html
Loyola University-Chicago	Access and Acceptable Use of University Computing, http://www.luc.edu/infotech/sae/newuse.html
	Bill of Rights and Responsibilities for the Electronic Community of Learners http://www.luc.edu/infotech/sae/bill-of-rights.html
University of Tulsa	Computer Ethics Code and Policy http://centum.utulsa.edu/ethics.html
Colgate University	Agreement for Use of Computing Facilities ftp://ftp.unm.edu/ethics/Colgate U.Policy
Indiana University	Computer Users' Privileges and Responsibility http://www.indiana.edu/~ucspubs/iu001/

(continued on next page)

Institution:	***Resource and URL Reference:***
Cornell University	Information Technology Rights and Responsibilities http://www.cornell.edu/Computer/responsible-use/Index.html#hate-speech Responsible Use of Electronic Communications http://www.univco.cornell.edu/policy/RU.for.html
University of California at Davis	Computer and Network Use Policy http://www.ucdavis.edu/AUP.html
University of Colorado	Administrative Policy Statement on the Use of E-mail http://www.cusys.edu/~policies/General/email.html
Dartmouth College	Computer and Network Policy http://www.dartmouth.edu/comp/comm/citbook/compcode.html
James Madison University	Appropriate Use of Information Technology Resources http://www.jmu.edu/JMUpolicy/1207.htm
Nassau Community College	Index of Polices: Select labpol.htm for Acceptable Use Policy for Computer Facilities http://www.sunynassau.edu/policies/labpol.htm
Notre Dame University	Responsible Use of Information Technologies at Notre Dame http://www.nd.edu/~doc/General/G0001.HTML
University of Pittsburgh	Computer Access and Use http://www.pitt.edu/DOC/94/271/42590/policies/10/10-02-05.html
University of Missouri-Columbia	Policies for Computer Use http://www.missouri.edu/iats/faculty/policies.shtml
Florida Atlantic University	Netiquette Home Page http://rs6000.adm.fau.edu/rinaldi/netiquette.html
University of Delaware	Policy for Responsible Computing http://www.udel.edu/eileen/Ecce/policy.approved.html
Brigham Young University	Computing/Network Patron Policies and Guidelines http://www.byu.edu/cougarnet/policy.html

*Note: This listing of Computer Access URLs can also be found on the NACUA homepage, using the following URL, user name and password:

URL: http://www.nacua.org/onlinepubs/access/chart.html
username: access
password: einstein

Be sure that these are typed exactly as above (lowercase).

Also Available from NACUA

Pamphlets/Monographs

Understanding Attorney-Client Privilege in the College and University Setting. *$12.00*
Access to Institutions of Higher Education for Students with Disabilities. *$12.00*
Accommodating Faculty and Staff with Psychiatric Disabilities. *$12.00*
Ownership and Retention of Data. *$7.50*
How to Conduct a Sexual Harassment Investigation. *$7.50*
A Guide to Copyright Issues in Higher Education. *$15.00*
Minority-Targeted Admissions and Financial Aid Programs. *$10.50*
Defamation Issues in Higher Education. *$7.50*
The Permissibility of Withholding Transcripts Under Bankruptcy. *$4.50*
The Family Medical Leave Act of 1993: Applications in Higher Education. *$6.50*
Looking a Gift Horse in the Mouth. *$6.50*
Acquaintance Rape on Campus: A Model for Institutional Response. *$12.50*
Managing Federal Student Financial Aid Programs. *$9.50*
Responding to Whistleblowers. *$6.50*
What to Do When OSHA Comes Calling. *$6.50*
Crime on Campus. *$9.50*
Risky Business: Risk Management, Loss Prevention and Insurance Procurement. *$6.50*
Peer Review Confidentiality: Is It Still Possible? *$6.50*
Technology Transfer and Risk Management. *$6.50*
Complying with "Drug-Free Workplace" Laws. *$6.50*
All Pamphlets and Monographs (a *$172.00* value) *$155.00*

Compendia

Sexual Harassment on Campus, Third Edition. *$40.00*
Student Disciplinary Issues, Second Edition. *$45.00*
Accommodating Students with Learning and Emotional Disabilities. *$42.50*
Employment Issues in Higher Education. *$37.50*
A Practical Guide to Title IX: Law, Principles, and Practices. *$42.50*
Title IX Gender Equity Athletic Program In-House Audit. *$15.00*
AIDS on Campus. *$20.00*
Academic Program Closures. *$29.50*
Regulating Racial Harassment on Campus. *$20.00*
Practical Aspects of Technology Transfer. *$20.00*
Record-Keeping and Reporting Requirements for Independent and Public Colleges and Universities. *$30.00* member institutions; *$60.00* non-member institutions
Instructional Supplement to *The Law of Higher Education*. *$45.00*
1997 Supplement to *The Law of Higher Education*. *$40.00*
Am I Liable? *$25.00*
Legal Issues in Faculty Employment. *$18.00*
Student Legal Issues. *$18.00*
Legal Issues in Athletics. *$18.00*

To receive a NACUA Publications Brochure with detailed descriptions of the resources listed above or to place an order:

- *write: NACUA Publications, One Dupont Circle, Suite 620, Washington, D.C. 20036*
- *e-mail: nacua@nacua.org, or*
- *visit our homepage: http://www.nacua.org*

PREPAID ORDERS ONLY.

National Association of College
and University Attorneys
One Dupont Circle, N.W.
Suite 620
Washington, D.C. 20036
202-833-8390
FAX 202-296-8379
http://www.nacua.org

NOTE TO ALL PURCHASERS OF:

Computer Access: Selected Legal Issues Affecting Higher Education:

The author has updated this publication to include the following three inserts. The two narrative additions have been incorporated directly into the on-line version, and the additional URL for the University of Georgia has been added to the electronic list of "Institutional Resources Accessible by URL" (see page 20 for the username and password).

(Page 8, preceding the section, "What is Due Process?"):

While private institutions are not constrained by due process considerations when drafting access policies, they, as well as public institutions, need to be mindful of guiding principles developed by the American Association of University Professors (AAUP). "Academic Freedom and Electronic Communications," an AAUP report, lists various principles reflecting *transcendent values of academic freedom* that apply to both public and private institutions. AAUP stresses the importance of academic freedom, inquiry, and freedom of expression that apply to both public and private institutions...*even though formal constraints...may apply only to publicly-supported colleges and universities* (http://www.aaup.org/statelec.htm).

The cited AAUP report provides guidance for all institutions when drafting computer access policies, including the following topics:

1. Freedom of Research and Publication.
2. Freedom of Teaching.
3. Access to the System: Acceptable Use Policies.
4. Responsibility in Extramural Utterances.
5. Avoiding Unwarranted Inference of Speaking for the Institution.
6. Sanctions: Terminating Access to the Network or System.
7. Freedom of Artistic Expression.
8. Campus Speech Codes and Harassment Rules.
9. Privacy of Electronic Communications.

For a rich discussion about academic freedom and the need for free artistic expression, see Marjorie Heins' article in the May-June 1998 issue of *Academe* entitled, "Academic Freedom and the Internet."

* *

(Page 14 after fn 57):

A nagging question for system administrators is whether it is possible to monitor and exercise editorial control without incurring distributor liability. The case of *Blumenthal v. Drudge and AOL* (922 F. Supp. 44 (1998)) may provide some helpful guidance. In this lawsuit,

Sidney and Jacqueline Blumenthal brought a defamation action against Matt Drudge, an electronic journalist, and American Online, Inc., an Internet Service Provider. The Blumenthals claimed that AOL was responsible for the alleged defamatory statements made by Drudge and then made available by AOL to its subscribers. Matt Drudge entered into a licensing agreement with AOL in which the Drudge Report was made available to AOL users. AOL, in turn, paid Drudge a royalty of $3,000/month. In its ruling, the Court noted that AOL was not a passive conduit like a telephone company, nor was it, in the Court's estimation, a common carrier with no control and, therefore, no responsibility for what is stated over the telephone wires. Noting that AOL had the right to exercise editorial control over those with whom it contracted and whose words it disseminated, the Court thought that it may seem fair to hold AOL liable. However, the Court also held that Congress created a different standard when it granted immunity for Internet Service Providers under the Communications Decency Act in an effort to provide an incentive for self-policing. (*Id.* at 51).

* *

University of Georgia
Policies on Use of Computers
http://www.uga.edu/~compsec/use.html